IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): A. Satoh et al.
Docket No.: JP920020242US1
Serial No.: 10/762,174
Filing Date: January 21, 2004
Group: 2193
Examiner: Tan V. Mai

Title: Multiplier and Cipher Circuit

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants (hereinafter referred to as "Appellants") hereby appeal the final rejection of claims 1-13 of the above-identified application.

The present application should be permitted to proceed to the Board for a decision on the merits.

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, as evidenced by an assignment recorded May 18, 2004 in the U.S. Patent and Trademark Office at Reel 14647, Frame 340. The assignee, International Business Machines Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any related appeals or interferences.

STATUS OF CLAIMS

The present application was filed on January 21, 2004 with claims 1-13.

Claims 1, 5, 9, and 13 are the pending independent claims.

Claims 1, 3, and 4 stand rejected under 35 U.S.C. §102(b).

Claims 2 and 5-13 stand rejected under 35 U.S.C. §103(a).

Claims 1-13 are appealed.

STATUS OF AMENDMENTS

There has been no amendment filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a multiplier. The multiplier comprises a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form. The multiplier also comprises a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form. The Wallace tree block comprises a sum calculation block adding the partial products, and a carry calculation block adding carries generated by the sum calculation block.

An illustrative embodiment of the recited multiplier is described in the specification at, for example, page 9, lines 6-18, with reference to FIG. 7. The multiplier comprises a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form (e.g., Specification, pg. 7, lines 9-23; FIG. 2; FIG. 3; FIG. 7, block 110). The multiplier also comprises a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form (e.g., Specification, pg. 7, lines 10-12; Specification, pg. 9, lines 19-21; FIG. 7, block 120). The Wallace tree block comprises a sum calculation block adding the partial products (e.g., FIG. 7, block 111; Specification, pg. 9, lines 7-15; Specification, pg. 11, lines 19-26), and a carry calculation block adding carries generated by the sum calculation block (e.g., FIG. 7, block 112; Specification, pg. 9, lines 7-18; Specification, pg. 12, lines 1-5).

Independent claim 5 recites a multiplier multiplying two input values as objects of multiplication by calculating partial products for the two input values and adding the partial products using half adders and full adders. The multiplier comprises multiplication means for calculating a sum of the partial products and outputting the sum as a result of the multiplication in the case that the input values are elements in an extension field of two. The multiplier further comprises carry addition means for adding carries generated in the calculation of the multiplication means. And, addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as the result of the multiplication in the case where the input values are integers.

An illustrative embodiment of the recited multiplier multiplying two input values as objects of multiplication by calculating partial products for the two input values and adding the partial products using half adders and full adders is described in the specification at, for example, page 9, lines 6-18, with reference to FIG. 7. The multiplier comprises multiplication means for calculating a sum of the partial products and outputting the sum as a result of the multiplication in the case that the input values are elements in an extension field of two (e.g., Specification, pg. 11, lines 19-26). The multiplier further comprises carry addition means for adding carries generated in the calculation of the multiplication means (e.g., Specification, pg. 9, lines 7-18; Specification, pg. 12, lines 1-5). And, addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as the result of the multiplication in the case where the input values are integers (e.g., Specification, pg. 12, lines 6-16).

Independent claim 9 recites a cipher circuit. The cipher circuit comprises arithmetic means for performing arithmetic for encryption or decryption of data, and control means for controlling the arithmetic by the arithmetic means. The arithmetic means comprise a multiplier using half adders and full adders and comprises a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form, and a carry propagation adder converting a redundant binary number outputted from the Wallace tree block to a resulting product in two's complement form. The Wallace tree block comprises a sum calculation block adding the partial products, and a carry calculation block adding carries generated by the sum calculation block.

An illustrative embodiment of the recited cipher circuit is described in the specification at, for example, page 14, lines 9-17, with reference to FIG. 11. The cipher circuit comprises arithmetic means for performing arithmetic for encryption or decryption of data (e.g., Specification, pg. 14, line 18, to pg. 15, line 10), and control means for controlling the arithmetic by the arithmetic means (e.g., Specification, pg. 14, lines 11-24). The arithmetic means comprise a multiplier using half adders and full adders (e.g., Specification, pg. 14, lines 24-25; and Specification, pg. 9, lines 6-18, with reference to FIG. 7) and comprises a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form (e.g., Specification, pg. 7, lines 9-23; FIG. 2; FIG. 3; FIG. 7, block 110), and a carry propagation adder converting a redundant binary number outputted from the Wallace tree block to a resulting product in two's complement form (e.g., Specification, pg. 7, lines 10-12; Specification, pg. 9, lines 19-21; FIG. 7, block 120). The Wallace tree block comprises a sum calculation block adding the partial products (e.g., FIG. 7, block 111; Specification, pg. 9, lines 7-15; Specification, pg. 11, lines 19-26), and a carry calculation block adding carries generated by the sum calculation block (e.g., FIG. 7, block 112; Specification, pg. 9, lines 7-18; Specification, pg. 12, lines 1-5).

Independent claim 13 recites a cipher circuit. The cipher circuit comprises arithmetic means for performing arithmetic for encryption or decryption of data, and control means for controlling the arithmetic by the arithmetic means. The arithmetic means comprises a multiplier which multiplies two input values as objects of multiplication by calculating partial products for the input values and adding the partial products using half adders and full adders. The arithmetic means comprises multiplication means for calculating a sum of the partial products for each digit and outputting the sum as a result of the multiplication in the case that the input values are elements of a finite field $GF(2^n)$; carry addition means for adding carries generated in the calculation of the multiplication means; and addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as a result of the multiplication in the case where the input values are integers.

An illustrative embodiment of the recited cipher circuit is described in the specification at, for example, page 14, lines 9-17, with reference to FIG. 11. The cipher circuit comprises

arithmetic means for performing arithmetic for encryption or decryption of data (e.g., Specification, pg. 14, line 18, to pg. 15, line 10), and control means for controlling the arithmetic by the arithmetic means (e.g., Specification, pg. 14, lines 11-24). The arithmetic means comprises a multiplier which multiplies two input values as objects of multiplication by calculating partial products for the input values and adding the partial products using half adders and full adders (e.g., Specification, pg. 14, lines 24-25; Specification, pg. 9, lines 6-18, with reference to FIG. 7; Specification, pg. 7, lines 9-23). The arithmetic means comprises multiplication means for calculating a sum of the partial products for each digit and outputting the sum as a result of the multiplication in the case that the input values are elements of a finite field $GF(2^n)$ (e.g., Specification, pg. 11, lines 19-26); carry addition means for adding carries generated in the calculation of the multiplication means (e.g., Specification, pg. 9, lines 7-18; Specification, pg. 12, lines 1-5); and addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as a result of the multiplication in the case where the input values are integers (e.g., Specification, pg. 12, lines 6-16).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 1, 3, and 4 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,847,981 (hereinafter "Kelley").

II. Claims 2 and 5-13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Kelley.

ARGUMENT

Appellants incorporate by reference herein the disclosures of a previous response filed in the present application, dated July 24, 2007. Sections I and II to follow will respectively address grounds I and II presented above.

I. Anticipation of claims 1, 3, and 4

Regarding the §102(b) rejection of claims 1, 3, and 4 based on Kelley, Appellants respectfully assert that Kelley fails to teach or suggest all of the limitations in claims 1, 3, and 4, for at least the reasons presented below.

Appellants initially note that it is well-established law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Appellants respectfully traverse the §102(b) rejection on the ground that the Kelley reference fails to teach or suggest each and every limitation of claims 1, 3, and 4 as alleged.

Independent claim 1 is directed to a multiplier, comprising: a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form; and a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form, wherein the Wallace tree block comprises: a sum calculation block adding the partial products, and a carry calculation block adding carries generated by the sum calculation block.

In the Office Action dated April 24, 2007, the Examiner states the following in formulating the rejection of claims 1, 3, and 4:

> As per independent claim 1, Kelley et al teach, e.g., see Figs. 3-8, the claimed combination. The circuit comprises "...reduction tree" (element 524 of Fig. 3), sum register (530) and (carry register (535) and adder (560). Also, see col. 1, line 63 to col. 2, line 44 [for Wallace tree], and col. 6 line 45 to col. 7, line 9, especially lines 45-54, i.e., "accumulated sum" and "accumulated carry" for the claimed "sum calculation block" and "carry calculation block", respectively.
>
> As per dependent claims 3-4, Kelley et al teach the detail features.

Appellants initially note that the Examiner has failed to provide any clear explanation of the reasoning in reaching the conclusion that the claims are anticipated by the cited reference (e.g.,

indicating the specific portions of Kelley which the Examiner believes anticipates each limitation of the claims). With regard to independent claim 1, the Examiner simply presents key words, cites general text, and cites blocks in figures without explaining with specificity how the cited reference anticipates the claim. And with regard to claims 3 and 4, the Examiner simply argues that Kelley teaches the claimed limitations. Appellants respectfully submit that the Office Action therefore fails to comply with 35 U.S.C. 132(a) ("Whenever, on examination, any claim for a patent is rejected, or any objection or requirement made, the Director shall notify the appellant thereof, stating the reasons for such rejection, or objection or requirement, together with such information and references as may be useful in judging of the propriety of continuing the prosecution of his application."); 37 CFR 1.104(c)(2) ("In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the appellant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified."); and MPEP 706.02(j) ("Where a reference is relied on to support a rejection, whether or not in a minor capacity, that reference should be positively included in the statement of the rejection. See In re Hoch, 428 F.2d 1341, 1342 n.3 166 USPQ 406, 407 n. 3 (CCPA 1970). It is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the appellant can be given fair opportunity to reply.")

Appellants further submit that Kelley fails to anticipate the claimed limitations. More specifically, Kelley does not teach a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form as recited in claim 1. Further, Kelley does not teach a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form as recited in claim 1.

Figure 4 of Kelley depicts an adder 560. However, no where does Kelley teach or suggest the adder converting a redundant binary number outputted from the Wallace tree block into a two's complement form. The only reference to "two's complement" is found at Kelley, col. 6, lines 17-22:

> [W]hen the values of a(i) or b(i), or both, have slight restrictions placed on them, such as when the a(i) or b(i), or both, are two's complement numbers, and a(i) and b(i), or both, never have a maximum negative value, the number of bits in one or both of the sum register 580 and the carry register 585 can designed to be yet one bit smaller.

Appellants respectfully contend that the Examiner has yet to cite a portion of Kelley that teaches a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form.

In response to this argument, the Examiner argues in the Final Office Action that "it is well known in the art that an adder, e.g., adder 740 of Fig. 3, which combines the results of "sum calculation block" and "carry calculation block" to provide the final result in two's complement form if one of operand a(i) / b(i) is two's complement number." Final Office Action, page 3, second full paragraph. First, Appellants submit that the Examiner is conceding that Kelley does not teach the claimed limitations because the Examiner is now combining Kelley with official notice. Furthermore, in response to this new argument, Appellants note MPEP 2144.03(a) which states that "[i]t is never appropriate to rely solely on 'common knowledge' in the art without evidentiary support in the record, as the principal evidence upon which a rejection was based. Zurko, 258 F.3d at 1385, 59 USPQ2d at 1697 ("[T]he Board cannot simply reach conclusions based on its own understanding or experience-or on its assessment of what would be basic knowledge or common sense. Rather, the Board must point to some concrete evidence in the record in support of these findings."). The Examiner has not presented any concrete evidence supporting the newly raised argument of "well known in the art" and, therefore, the Examiner's rejection is without merit.

Next, Appellants respectfully submit that the Examiner's argument fails to support the anticipation rejection. Regardless of the fact that a final result of an adder may be in two's complement form if one of operand a(i) / b(i) are two's complement numbers, the Kelley reference does not teach a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form. Accordingly, it is believed that the teachings of Kelley fail to meet the limitations of claim 1.

It follows that dependent claims 3 and 4 recite patentable subject matter at least by virtue of their respective dependency from independent claim 1. Dependent claims 3 and 4 also recite patentable subject matter in their own right.

Dependent claim 3 recites that the carry propagation adder adds a result of the calculation of the sum calculation block and a result of the calculation of the carry calculation block and outputs a result of the addition as a result of the multiplication for integers. Dependent claim 4 recites that the sum calculation block performs multiply and add operations by adding another value for each corresponding digit to the partial products.

Appellants reiterate that the Examiner fails to argue with specificity the grounds for rejecting claims 3 and 4. In response to Appellant's contention, the Examiner states in the Final Office Action, page 3, fourth full paragraph, "in Kelley, the output of adder is actually the claimed 'result of the addition as a result of the multiplication for integers'." Appellants contend that the fact that the output of the adder is the result of the addition as a result of the multiplication for integers is irrelevant. Kelley does not teach that the carry propagation adder adds (1) a result of the calculation of the sum calculation block and (2) a result of the calculation of the carry calculation block and outputs a result of the addition as a result of the multiplication for integers.

Accordingly, Appellants believe that Kelley fails to anticipate the limitations of claims 3 and 4 and, therefore, respectfully request withdrawal of the §102 rejection.

II. Obviousness of claims 2 and 5-13

With regard to the §103(a) rejection of claims 2 and 5-13, Appellants initially note that a proper case of obviousness has not been presented if the references, when combined, do not teach or suggest all the claim limitations. Furthermore, the claimed subject matter is not obvious if there is no suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or to modify the reference teachings. An analysis supporting a rejection under 35 U.S.C. §103 should be explicit and should not based on mere conclusory statements. See KSR v. Teleflex, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements;

instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.").

With regard to claim 2, Appellants initially note that claim 2 is patentable due to its dependence from claim 1, the patentability of which was discussed above. Next, the Kelley reference, even if modified, fails to teach or suggest a result of the calculation of the sum calculation block is outputted as a result of the multiplication over an extension field of two, as recited in claim 2. The Examiner argues in the Final Office Action at page 3, third full paragraph, that:

> "result of the multiplication over an extension field of two" is merely a result of Galois field / finite field computation. Hansen et al (Ref. B) does Wallace tree technique, i.e., carry save, adder, in the Galois field and finite field.

Although Hansen mentions a Wallace tree and Galois fields, Appellants assert that Kelley combined with Hansen fails to teach that a result of the calculation of the sum calculation block (of the Wallace tree block recited in claim 1) is outputted as a result of the multiplication over an extension field of two.

Furthermore, the Examiner presents insufficient evidence for a motivation or suggestion to combine or modify the cited references. The Examiner argues in the Final Office Action, pg. 3, third full paragraph:

> Therefore, it would be obvious to a person having ordinary skill in the art to use to sum "portion" of the 4-2 ADD (Fig. 211) as the claimed "result of the multiplication over an extension field of two."

Appellants respectfully submit that this is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of objective evidence of record that would motivate one skilled in the art to combine Kelley with Galois field and finite field to produce the particular limitations in question.

With regard to the §103(a) rejection of claim 5, the Examiner refers to claim 5 as being similar to the combination of claims 2 and 3, and is thus rejected under a similar rationale. Appellants assert that claim 5 is patentable for at least the reasons discussed above with regard to claims 2 and 3.

With regard to claims 6-8, Appellants assert that the claims are patentable due to their dependence from claim 5, the patentability of which was discussed above. Further, in rejecting the claims, the Examiner simply states in the Office Action, page 4, paragraph six, that "the claims add the detail features which are obvious to a person having ordinary skill in the art." Appellants disagree and request that the rejection of claims 6-8 be withdrawn because the Examiner failed to submit evidence supporting this contention. Furthermore, Appellants respectfully submit that the Examiner's argument is another conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court.

With regard to the rejection of claims 9-13, Appellants initially submit that independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1. Further, independent claim 13 includes limitations similar to those of claim 5, and is therefore believed allowable for reasons similar to those described above with reference to claim 5. Also, dependent claims 10-12 recite patentable subject matter at least by virtue of their respective dependency from independent claims 1 and 9, and also recite patentable subject matter in their own right.

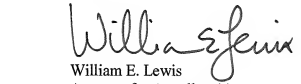
In rejecting claims 9-13, the Examiner argues in the Office Action, page 4, last paragraph, that "[i]t would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the multiplier circuit can be used in Galois field / finite field device as claimed." Appellants respectfully submit that this is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of objective evidence of record that would motivate one skilled in the art to combine Kelley with Galois fields and finite

fields to produce a cipher circuit as recited in the claims. Appellants respectfully contend that neither Kelley nor Hansen discuss a cipher circuit. Furthermore, the Examiner fails to explain with specificity how the combined references teach or suggest each and every claimed limitation.

For at least these reasons, Appellants request that the rejection of claims 2 and 5-13 be withdrawn.

In view of the above, Appellants believe that claims 1-13 are in condition for allowance, and respectfully request withdrawal of the §102(b) and §103(a) rejections.

Respectfully submitted,



Date: January 31, 2008

William E. Lewis
Attorney for Appellant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

APPENDIX

1. A multiplier, comprising:

a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form; and

a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form, wherein

the Wallace tree block comprises:

a sum calculation block adding the partial products, and

a carry calculation block adding carries generated by the sum calculation block.

2. The multiplier according to claim 1, wherein a result of the calculation of the sum calculation block is outputted as a result of the multiplication over an extension field of two.

3. The multiplier according to claim 1, wherein the carry propagation adder adds a result of the calculation of the sum calculation block and a result of the calculation of the carry calculation block and outputs a result of the addition as a result of the multiplication for integers.

4. The multiplier according to claim 1, wherein the sum calculation block performs multiply and add operations by adding another value for each corresponding digit to the partial products.

5. A multiplier multiplying two input values as objects of multiplication by calculating partial products for the two input values and adding the partial products using half adders and full adders, the multiplier comprising:

multiplication means for calculating a sum of the partial products and outputting the sum as a result of the multiplication in the case that the input values are elements in an extension field of two;

carry addition means for adding carries generated in the calculation of the multiplication means; and

addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as the result of the multiplication in the case where the input values are integers.

6. The multiplier according to claim 5, wherein the multiplication means collects and outputs only addition terms by an exclusive OR operation, addition terms being outputted from the half adders and the full adders.

7. The multiplier according to claim 6, wherein the carry adder means collects terms other than the addition terms added by the multiplication means and performs addition including the carry terms and the addition terms by the half adders and the full adders.

8. The multiplier according to claim 6, wherein a multiply and add operation is performed by adding the addition terms of the partial products in the multiplication means to other addition terms.

9. A cipher circuit, comprising:

arithmetic means for performing arithmetic for encryption or decryption of data; and

control means for controlling the arithmetic by the arithmetic means;

wherein the arithmetic means comprise a multiplier using half adders and full adders and comprises:

a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form; and

a carry propagation adder converting a redundant binary number outputted from the Wallace tree block to a resulting product in two's complement form; and

wherein the Wallace tree block comprises:

a sum calculation block adding the partial products, and

a carry calculation block adding carries generated by the sum calculation block.

10. The cipher circuit according to claim 9, wherein the arithmetic means outputs a result of the calculation of the sum calculation block in the case of arithmetic over a finite field

$GF(2^n)$ and outputs a result of the calculation of the carry calculation block in the case of arithmetic over a finite field GF(p).

11. The cipher circuit according to claim 9, wherein the sum calculation block collects and outputs only addition terms by an exclusive OR operation outside of the arithmetic means, the addition terms being outputted from the half adders and the full adders.

12. The cipher circuit according to claim 9, wherein the carry calculation block collects terms other than addition terms added by the multiplication means and performs addition including the carry terms and the addition terms by the half adders and the full adders.

13. A cipher circuit, comprising:

arithmetic means for performing arithmetic for encryption or decryption of data; and

control means for controlling the arithmetic by the arithmetic means;

wherein the arithmetic means comprises a multiplier which multiplies two input values as objects of multiplication by calculating partial products for the input values and adding the partial products using half adders and full adders and the arithmetic means comprises:

multiplication means for calculating a sum of the partial products for each digit and outputting the sum as a result of the multiplication in the case that the input values are elements of a finite field $GF(2^n)$; and

carry addition means for adding carries generated in the calculation of the multiplication means; and

addition means for adding a result of the calculation of the multiplication means and a result of the calculation of the carry addition means and outputting a result of the addition as a result of the multiplication in the case where the input values are integers.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.